XSS Vulnerability Report: emeroteca.braidense.it

Cross-Site Scripting (XSS) Vulnerability Report

Executive Summary

As part of a CyberSecurity homework task, I conducted an XSS vulnerability assessment on the website http://emeroteca.braidense.it/indice_testate.php. The assessment revealed a significant security flaw that allows for the injection of malicious scripts, potentially compromising user data and site integrity.

Target URL

http://emeroteca.braidense.it/indice_testate.php

Vulnerability Details

The website is vulnerable to Reflected Cross-Site Scripting (XSS) attacks. This vulnerability was discovered in the 'SearchString' parameter of the search functionality.

Proof of Concept

The following payload was successfully injected into the 'SearchString' parameter:

```
"><script>alert('XSS');</script>
```

Impact

This vulnerability could allow an attacker to:

- Steal user session cookies
- Perform unauthorized actions on behalf of the user
- Deface the website
- Redirect users to malicious websites

Remediation Steps

To address this vulnerability, the following steps are recommended:

- Implement proper input validation and sanitization for all user inputs
- Use content security policies (CSP) to prevent the execution of inline scripts
- Encode output data to prevent script execution in the browser
- Consider using frameworks or libraries that automatically escape user input

Conclusion

The discovered XSS vulnerability poses a significant risk to both the website and its users. Immediate action is recommended to patch this security flaw and prevent potential exploitation.